



The European B2B Forum for the Electronics Industry

EDIFICE Guideline

Internet EDI

Issue 1

Endorsed 16 June 1999

Copyright (c) EDIFICE 2004

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without prior permission of EDIFICE.

Notwithstanding the fact that the utmost care has been observed in the collecting, drawing up and formulating of data, EDIFICE can under no circumstances be held liable for errors, omissions or misinterpretations as a result of the information compiled in the guidelines.

EDIFICE
The European B2B Forum for the Electronics Industry
EDIFICE secretariat
Dora Cresens
Tiensestraat 2
B-3320 Hoegaarden
Belgium
Tel: +32 16 76 54 40
Fax: +32 16 76 53 58
Email: Dora.Cresens@edifice.org

Publication Summary

Title:	EDIFICE INTERNET EDI Implementation Guideline
Author (s):	EDIFICE Internet Group
Issue number:	Issue 1
Date of Issue:	16 June 1999
Number of Pages:	16
Readership:	Internet task group
Language:	English
Abstract:	This document provides guidance on implementation steps required to use the Internet for transport of EDI messages. Comments and change requests to this document should be submitted to: EDIFICE Internet Group
Comment:	@ EDIFICE secretariat
References	CommerceNet : http://www.commerceNet.com IETF : www.imc.org/ietf-ediint/ Requirements for Inter-operable Internet EDI : Draft 06

Table of Content

Comparison to previous issue.....	4
1 Introduction.....	4
1.1 Readership.....	4
1.2 EDI Internet standards.....	4
1.3 Overview of infrastructure.....	4
1.4 Comparison with UN/EDIFACT security.....	5
1.5 Business case.....	6
2 EDIFICE recommendations.....	8
2.1 Symmetric Encryption.....	8
2.2 Symmetric Key Management.....	8
2.3 Public and Private Keys.....	8
2.4 Trust and Public Keys.....	9
2.5 Content Integrity.....	9
2.6 Authentication and Non-Repudiation of Origin.....	9
2.7 Signed Receipt or Non Repudiation of Receipt.....	9
2.8 Syntax and Protocol for Specifying Cryptographic Services.....	9
2.9 Tracking and Error Handling Basics.....	9
2.10 Transmission Successfully Encoded, Encrypted, Signed and Sent.....	9
2.11 Transmission Successfully Delivered to the Recipient's.....	10
2.12 Transmission Successfully Received.....	10
2.13 Transmission Successfully Translated by the Receiver.....	10
2.14 Detection and Recovery of Delayed or Lost Transmissions.....	10
2.15 Detection and Handling of Duplicate Transmissions.....	10
3 Test results.....	10
Annex 1 : EDI Encryption process.....	11
Annex 2 : Initial/ongoing cost items for an EDI over Internet package/solution implementation.....	14
Annex 3 - Abbreviations/Glossary of terms.....	15

Comparison to previous issue

No existing previous issue.

1 Introduction

1.1 Readership

This document is intended to provide guidance to both the commercial and IT technical representatives of trading partners who intend to use the Internet as transport facility for EDIFACT EDI messages.

1.2 EDI Internet standards

Work has been done by an Internet Engineering Task Force (IETF) on standardising the approach to EDI over the Internet (EDIINT). Their documents and mailing list can be found at <http://www.imc.org/ietf-ediint/> . This EDIFICE guideline is based on the work of the IETF EDIINT.

1.3 Overview of infrastructure

Before any secured EDI messages may be transmitted over the Internet both yourselves and your trading partner must:

1. Own an encryption tool, which is interoperable according to the standards defined by IETF (Internet Engineering Task Force) and tested by CommerceNet.
2. Your trading partner and yourselves must have some transport mechanism in place for exchanging messages over an open network, such as Internet email.
3. Some EDI translator needs to be in place for processing EDI formatted messages such as EDIFACT or ANSI X12. The encryption tool only provides the transport of EDI formatted messages.
4. To run the encryption software a server will be necessary or a PC for smaller companies with little traffic.

For further information on encryption tool interoperability see <http://www.commerceNet.com>. Some of the companies participating in the CommerceNet testing are Harbinger, Netscape, Sterling Commerce, Cyclone Software, SAA Consultants, St Paul Software and Compaq's Tandem Group. This list may change. Refer to CommerceNet for the latest information.

Check the performance of your internet service provider (ISP) to ensure that the service is adequate to meet the needs of the business function which is to be supported by EDI over the Internet.

Transport over the Open Network consists of SMTP (Email), HTTP, HTTPS or FTP.

The recommendations of the IETF EDIINT provide various security services to be implemented between the EDI translator and the transport via Internet. The relationship between the application systems which are communicating and the various service components is shown in Figure 1.

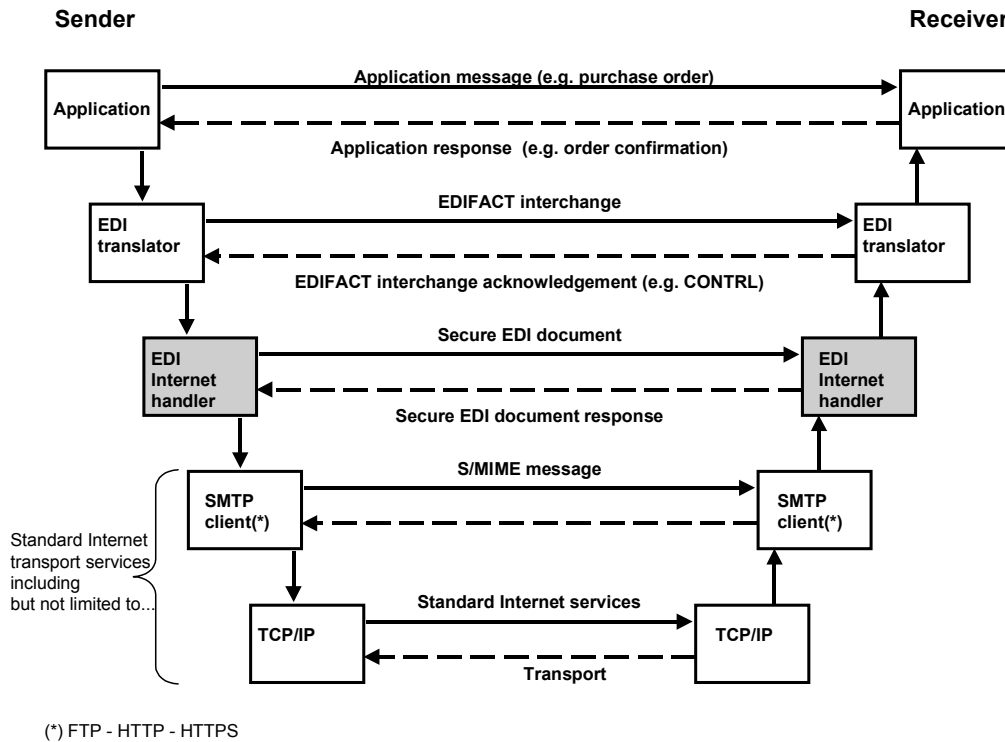


Figure 1 Overview of EDI Internet Infrastructure

This shows a layered architecture. For each layer the communication from sender to receiver is shown and the possible response, which forms part of the control mechanism for that layer, is also shown. Each layer is depending on the services of the next following lower layer.

The sender application system sends an application message (e.g. a purchase order) and may receive a response from the receiving application system (e.g. purchase order acknowledgement). The nature of the control loop in this layer depends on the type of application.

The EDI translator sends the application message in an EDIFACT interchange, and may receive a response to the interchange from the receiving EDI translator. Such a response merely acknowledges receipt of the EDIFACT interchange.

The EDI Internet handler sends the EDIFACT interchange in a secure EDI document and receives a secure response from the receiving EDI Internet handler. This guideline focuses on the various types of security services recommended for use in this layer.

The secure EDI document is sent via standard Internet transport services.

1.4 Comparison with UN/EDIFACT security

The IETF EDIINT specification applies to the EDI Interchange or Bundle (multiple EDI interchanges) level, and not to the message level.

Any security services, packaging, transport, or non-repudiation services are assumed to be applied to an entire EDI Interchange. This is unlike the UN/EDIFACT approach in the drafts for ISO 9735 syntax version 4 in parts 5 and 6 on security standards in which the security services can be applied within the EDIFACT interchange. The purpose of the IETF

EDIINT specification is to move these services out of the translator, and into the communications subsystem. The communications subsystem should know as little about the structure of the EDI data as possible. The entire EDI Interchange, including the envelope headers (UNA/UNB/UNZ) are encrypted, when encryption security services are applied. Since the routing of the EDI Interchange is through the Internet, and not a VAN, the sender/receiver ids in the UNB are not used in mailbox routing.

1.5 Business case

In recent years value added network services (VANS) have been the normal means used for transport of EDI messages. The Internet is now seen as an alternative. This section provides an overview of the pros and cons of using the Internet as alternative to a VAN. This overview can be used as the basis for building a business case for a specific situation.

PROs	CONs
Cost benefit vs. VANS	Admin costs certificate management partner profiles
Access to smaller partners	No VAN for logging backup and recovery
Flexibility - access to all	Technical problems of security implementation
Leverage of common use of TCP/IP infrastructure	Legal restrictions
Offers the possibility of event driven "push" vs. VAN batch "pull"	Network reliability & speed in certain countries
Proven demonstrable security	
Security facility available to all communications - e-mail, etc.	

LEGAL AND FISCAL STATUS

Surveys of the legal and fiscal status for the use of EDI over Internet in the main countries in Europe have shown that it is possible to use this procedure. However, it is advisable to consult your local legal authorities before you implement the EDI over Internet procedure.

TRADING PARTNER AGREEMENT

It is also advisable to make an agreement with your EDI over Internet trading partner. Following are the questions that need to be agreed upon:

Questions to ask your Trading partner:	
COMPANY	
Company name	
Contact Name, number, fax number and E-mail address	
Address	
PRODUCTION EDI system email address (system where EDI messages and public key are to be sent to)	
TEST EDI system email address (system where EDI messages and public key are to be sent to)	
UNB/ISA ID	
UNB/ISA qualifier	
Test ID and qualifier, if different	
Encryption	
Encryption Tool used (ensure the tool is interoperable) Name:	
Version:	
Is encryption required?	
Will digital signatures be exchanged?	
What digital signature algorithm is to be used, MD5 or SHA-1?	
Public/Private key size? (e.g. 1024 bit)	
Version (X.509v):	
Single key encryption to be used (e.g. RC2 128 bit)	
Are MDNs (Message Disposition Notifications) required?	
Will S/MIME enveloping be used?	
Version:	
Method of certificate exchange (email, diskette, FTP,...) ?	
Certificate Expiration date?	
Transport-FTP	
IP address/host name	
User ID	
Password	
Destination folder	
Port Number	
Transport – HTTP/HTTPS	
Host name	
Port Number	
Transport - SMTP	
Is there a limit to size of messages within the trading partners or your email gateway?	
What is the time frame before acknowledgements are sent?	

The same details on your company will need to be given to your trading partner.

If you want to make use of Trading Partner agreement, there is a European Model EDI agreement on the web at : <http://www.edifice.org/secure/agree.pdf>

2 EDIFICE recommendations

The recommendations made are based primarily on a draft document produced by the Internet Engineering Task Force (IETF) EDIINT Working Group on inter-operable Internet EDI. These drafts have been produced by 'experts' in their field and there seems little point in the EDIFICE EDI Over the Internet (EOI) work group trying to re-invent the wheel, but rather to leverage as much as we can from the wealth of experience and knowledge contained in these documents. The IETF document like all drafts should be considered as 'Work In Progress' and as quoted by the IETF are

'... valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time'

At the time of writing the most current document available is **draft-ietf-ediint-req-06.txt** (expiration date June 99) and can be downloaded from: <ftp://ftp.nordu.net/internet-drafts>(Northern Europe) or <ftp://ftp.garr.net/doc/internet-drafts/> (Southern Europe).

Also stored on the EDIFICE web : <http://www.edifice.org/ietf06.txt>

For EDIFICE members looking at EOI, this sections attempts to provide some guidance, such that those taking on board the recommendations made in this paper will not only be standardising on inter-operable methods for doing EDI over the Internet but also positioning themselves for undertaking all kinds of secure business messaging.

For each of the EDI issues tackled there is an abbreviated description of the need along with an accompanying reference (Ref:) to where the full text can be found in the IETF document.

2.1 Symmetric Encryption

(Ref: Section 3.2.6)

Symmetric encryption (also called single key encryption) is the fastest form of encryption and is generally used to encrypt the body of the message itself using a randomly generated key. The same key is used to encrypt and de-encrypt the message.

In order to provide confidentiality for EDI Interchanges on the Internet between two trading partners, the encryption algorithm and key lengths must be agreed upon either before hand, or within an individual transaction.

EDIFICE recommends that the main body of the message should be encrypted using symmetric encryption.

2.2 Symmetric Key Management

(Ref: Section 3.3.4)

The keys used for symmetric encryption need to be passed to the message recipient in a secure manner.

EDIFICE recommends that keys should be issued on a per transaction basis (so called 'session keys').

Symmetric keys should be protected by public key encryption.

2.3 Public and Private Keys

(Ref: Section 3.4.2)

Public and private keys are used to provide Asymmetric encryption, which provides a higher level of security. These are the keys used to protect the symmetric keys and provide the security for receipts etc. The longer the key, the greater the security.

2.4 Trust and Public Keys

(*Ref: Section 3.4.6.1*)

The method of ensuring that a given 'key' belongs to a specified person is called a trust model. Certified keys can be commercially provided through certification authorities, or can be on a self-certification basis.

2.5 Content Integrity

(*Ref: Section 3.5.4*)

There is a need to ensure the integrity of a message. Normally a checksum or hash is calculated and included in the transmission.

2.6 Authentication and Non-Repudiation of Origin

(*Ref: Section 3.6.4*)

There is a need to ensure the origin of a message, this is normally accomplished by the use of a digital signature.

2.7 Signed Receipt or Non Repudiation of Receipt

(*Ref: Section 3.7.3*)

There needs to be a method of providing guarantee of receipt of a message, this is provided by a digitally signed receipt.

EDIFICE recommends that signed receipts should be used.

2.8 Syntax and Protocol for Specifying Cryptographic Services

(*Ref: Section 3.8.4*)

A syntax and protocol for specifying EDI Interchanges that have had cryptography applied to them, needs to be specified. Several suitable standards already exist, so it is preferable to choose one of these existing standards rather than specifying a new one.

2.9 Tracking and Error Handling Basics

(*Ref: Section 4.2.2*)

There needs to be a facility by which a sender can be assured that the EDI transmission was correctly translated and prepared for outbound transmission.

2.10 Transmission Successfully Encoded, Encrypted, Signed and Sent

(*Ref: Section 4.3.2*)

There needs to be a facility by which a sender can be assured that an EDI transmission was successfully encoded, encrypted, signed, and sent.

2.11 Transmission Successfully Delivered to the Recipient's

(Ref: Section 4.4.2)

There needs to be a facility by which a sender can be assured that an EDI transmission was successfully delivered to a recipient's mailbox.

2.12 Transmission Successfully Received

(Ref: Section 4.5.2)

There needs to be a facility by which a sender of a transmission can be assured that the transmission was correctly received by the intended receiver.

2.13 Transmission Successfully Translated by the Receiver

(Ref: Section 4.6.2)

There needs to be a facility for the sender to be assured that the receiver could "understand" (in EDI terms) the transmission.

2.14 Detection and Recovery of Delayed or Lost Transmissions

(Ref: Section 4.7.2)

There needs to be a facility by which a sender can detect sent transmissions that have not been acknowledged as correctly received, by a specified, configurable, period of time, and be able to configure actions accordingly.

EDIFICE recommends that signed receipts should always be requested.

2.15 Detection and Handling of Duplicate Transmissions

(Ref: Section 4.8.2)

There needs to be a facility by which a receiver of EDI transmissions is able to detect different types of duplicate transmissions, and handle them correctly. First, translator initiated duplicates SHOULD NOT be halted in any way - it should be assumed that translators will handle that level of duplication. In other words, there should be no checking of X12 ISA control numbers or EDIFACT UNB Interchange Control Reference by the UA. Secondly, the use of a re-transmission feature in attempts to deliver transmissions quickly, should allow for a UA to identify duplicate transmissions generated by the sending UA, and discard the duplicate transmissions after the first has been received.

3 Test results

The results of tests by EDIFICE members can be found at the following Internet addresses:

Texas Instruments: <http://www.edifice.org/secure/intti.pdf>

Motorola : <http://www.edifice.org/secure/intmot.pdf>

STMicroelectronics: <http://www.edifice.org/secure/intst.pdf>

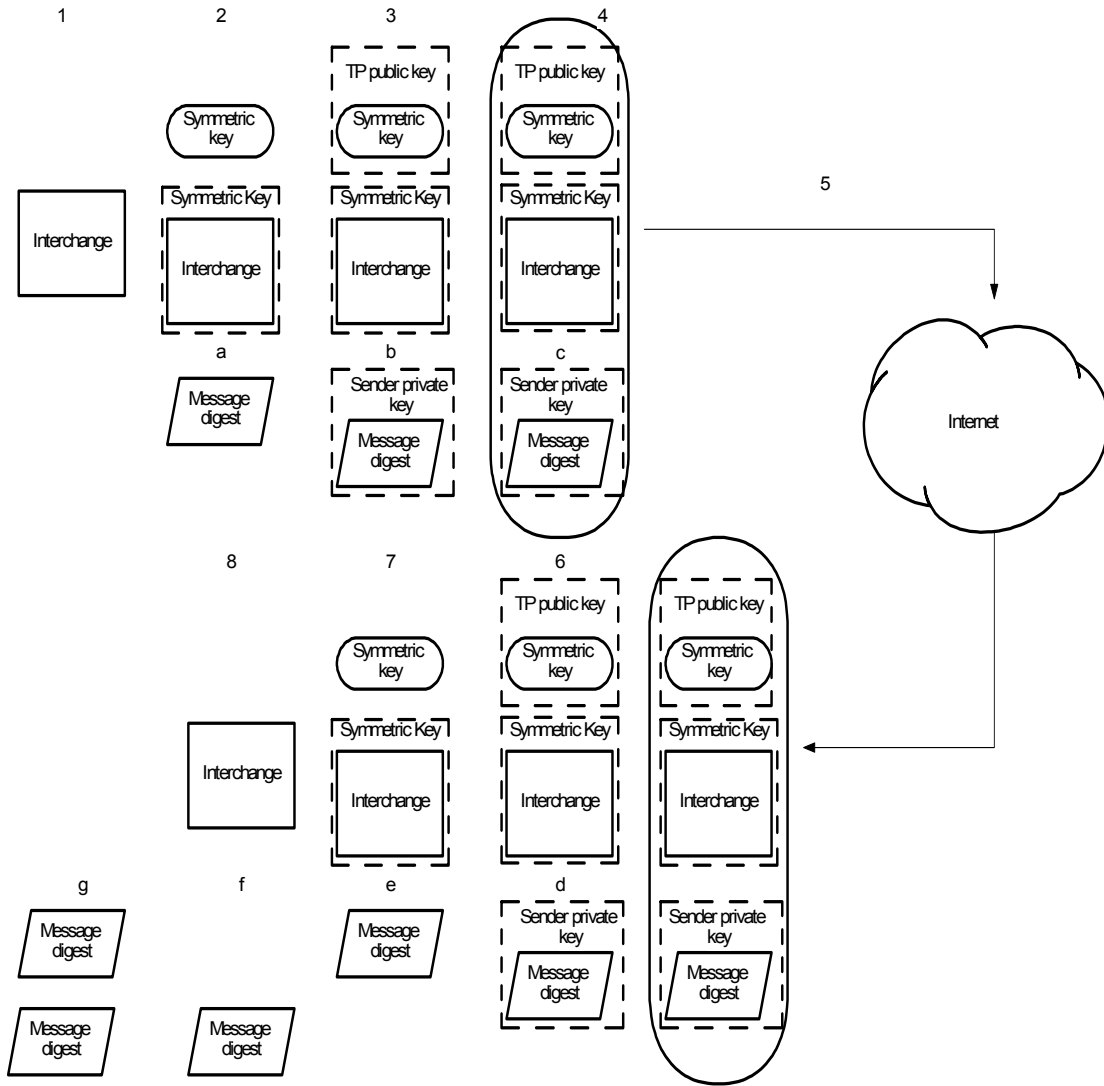
Annex 1 : EDI Encryption process

Interchange encryption process: To insure confidentiality

- 1) The EDI translator generates the interchange
- 2) The EDI Internet Handler randomly generates a symmetric key.
The Interchange is encrypted with the symmetric key. This insures the confidentiality.
- 3) The symmetric key is encrypted using the Trading Partner's public key (Asymmetric)
- 4) The EDI Internet Handler encloses the encrypted EDI interchange and the encrypted symmetric key in a S/MIME envelope.
- 5) The EDI Internet Handler sends the envelope to the Trading Partner over the Internet.
- 6) The S/MIME envelope is removed
- 7) The Trading Partner uses his private key (Asymmetric) to decrypt the received symmetric key.
- 8) The symmetric key is used to decrypt the interchange.

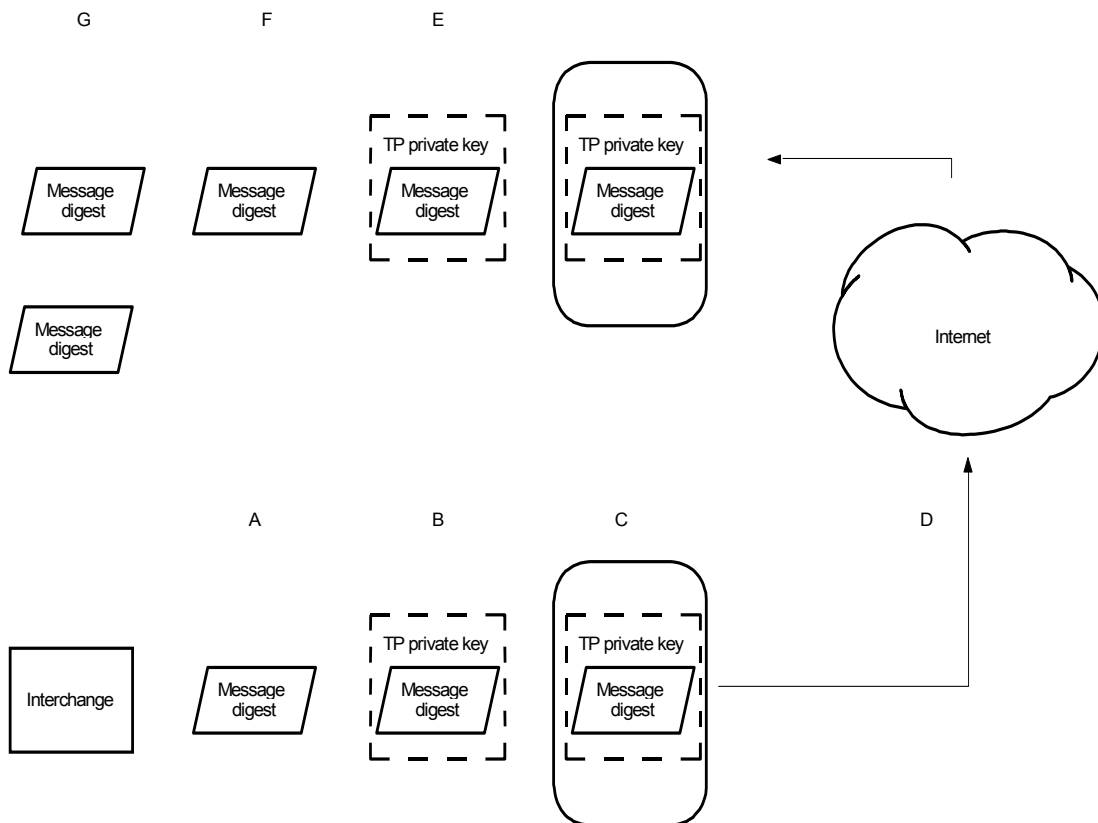
Digital signature process: To insure Integrity, Authentication and Non Repudiation of Origin

- a) The EDI Internet Handler generates a Message Digest
- b) The EDI Internet Handler uses the sender private key (Asymmetric) to encrypt the Message Digest
- c) The encrypted Message Digest is included in the S/MIME envelope
- d) The encrypted Message digest is extracted from the S/MIME envelope
- e) The receiving EDI Internet Handler uses the public key (Asymmetric) of the sender to decrypt the Message digest. The sender is identified.
- f) The receiving EDI Internet Handler generates a new Message Digest from the decrypted interchange
- g) The two Message Digest's are compared to check the integrity of the interchange



Acknowledgement process: To insure the Non Repudiation of Receipt and the Integrity of received interchange

- A) The Trading Partner generates a Message Digest of the received interchange.
- B) The Trading Partner signs the Message Digest by encrypting it with its private key (Asymmetric).
- C) The Trading Partner's EDI Internet Handler enclosed the encrypted Message Digest in a S/MIME envelope.
- D) The Trading Partner's EDI Internet Handler sends the envelope to the original interchange sender.
- E) The S/MIME envelope is removed
- F) The EDI Internet Handler uses the Trading Partner's public key (Asymmetric) to decrypt the Message Digest. The receiver is identified.
- G) The decrypted Message Digest is compared with the original interchange Message Digest, to check the integrity of the received interchange.



Annex 2 : Initial/ongoing cost items for an EDI over Internet package/solution implementation

INITIAL INVESTMENT

TOPIC	DESCRIPTION
SOFTWARE	<ul style="list-style-type: none"> • EOI product licenses acquisition <ul style="list-style-type: none"> ☞ server product, clients... • Maintenance • Additional developments <ul style="list-style-type: none"> ☞ Translator interfaces...
HARDWARE	<ul style="list-style-type: none"> • Computers <ul style="list-style-type: none"> ☞ PCs, mail server, disks... • Firewall • Network interface devices • Network cabling • Special peripherals <ul style="list-style-type: none"> ☞ Tape backup systems...
MISCELLANEOUS	<ul style="list-style-type: none"> • Consulting <ul style="list-style-type: none"> ☞ Internet security, key management... • Users training • Software installation

ONGOING/RECURRING COSTS

TOPIC	DESCRIPTION
OPERATIONS	<ul style="list-style-type: none"> • Technical support <ul style="list-style-type: none"> ☞ Mailbox, Software processes, Internet gateway, Interfaces • Administration <ul style="list-style-type: none"> ☞ TP profiles, agreements, key management
HARDWARE/ COMMUNICATION	<ul style="list-style-type: none"> • Hardware depreciation • Internet communication
SOFTWARE	<ul style="list-style-type: none"> • Software maintenance <ul style="list-style-type: none"> ☞ Upgrades, additional developments...

Annex 3 - Abbreviations/Glossary of terms

Authentication	A process that ensures that the receiver of a message can be confident of the identity of the sender and the integrity of the data in the message.
Certificate	A digital document that attests to the binding of a public key to an organisation. It verifies that a public key belongs to a given organisation.
Digital signature	A character string that cannot be forged. Digital signatures are used in the nonrepudiation of origin and receipt security features.
EDI	Electronic Data Interchange
EDI Interchange	A group of documents electronically exchanged as a unit between two trading partners.
EDI Internet Handler	Middleware, which is situated between an EDI translator and the Internet, to provide the security functions for transport of EDI interchanges according to the IETF EDIINT recommendations.
EDIINT	EDI over the Internet
Encryption	The transformation of data into a form that is unreadable by anyone who does not have the key to decrypt it. Encryption ensures that documents exchanged between trading partners over a public network remain private.
EOI	EDI Over the Internet
FTP	File Transfer Protocol. A format for transmitting files from your computer to your trading partner's FTP server.
HTTP	Hypertext Transfer Protocol. HTTP is a communication protocol used to connect to servers on the World Wide Web.
HTTPS	Secure HTTP
IETF	Internet Engineering Task Force
Interoperable	UAs in a communications network which function compatibly according to a given specification.
ISP	Internet Service Provider
IP address	The address of a network interface
MDN	Message Disposition Notification. A MIME-based receipt providing authentication and acknowledgement that a message was received. An MDN reports the status of the decryption, authentication, and integrity of the data

received. A signed MDN provides nonrepudiation of receipt.

Message digest	The result of a computation that takes a variable-sized set of data and returns a fixed-sized character string, the message digest. This message digest is a mathematical summary of the data used in its calculation.
MIME	Multipurpose Internet Mail Extensions. MIME is a standard for formatting messages. It provides standard methods for encoding binary data, multipart messages and data type labelling and message fragmentation.
Nonrepudiation of origin	A security feature that verifies the identity of the sender of an EDI Interchange and the integrity of its contents.
Nonrepudiation of receipt	A security feature that verifies to the sender that the receiver of a message received the message and that the integrity of its contents was not compromised.
Private key	In public/private key cryptography, the key in a public/private key pair that is never exchanged between trading partners or published.
Public key	In public/private key cryptography, the key in a public/private key pair that is exchanged between trading partners and published.
S/MIME	Secure/Multipurpose Internet Mail Extensions. S/MIME is a specification for secure electronic mail. It uses digital signatures and encryption to add security to e-mail messages in MIME format.
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol. TCP/IP is a set of communication protocols that support direct communication links with local- and wide-area networks.
UA	User Agent
UN/EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
VAN	Value Added Network